IN THE CLAIMS:

Please amend the claims as follows:

1. (canceled)

2. (canceled)

B1

1. (previously presented) A cryptographic key split combiner, comprising:

a plurality of key split generators for generating cryptographic key splits; and

a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key;

wherein each of said key split generators includes means for generating key splits from seed data;

wherein said plurality of key split generators includes a random split generator for generating a random key split based on reference data; and

wherein said random split generator includes means for generating a random sequence based on the reference data.

2. (previously presented) The cryptographic key split combiner of claim 1, wherein said random split generator includes means for generating a pseudorandom sequence based on the reference data.

3. (previously presented) The cryptographic key split combiner of claim 1, wherein said random split generator includes means for generating a key split based on the reference data and on chronological data.

4. (previously presented) The cryptographic key split combiner of claim 1, wherein said random split generator includes means for generating a key split based on the reference data and on static data.

5. (original) The cryptographic key split combiner of claim 4, further including means for updating the static data.

6. (original) The cryptographic key split combiner of claim 5, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

7. (previously presented) The cryptographic key split combiner of claim 1, wherein said plurality of key split generators includes a token split generator for generating a token key split based on label data.

8. (original) The cryptographic key split combiner of claim 7, further comprising means for reading the label data from a storage medium.

9. 7
11. (original) The cryptographic key split combiner of claim ~~9~~, wherein the label data includes user authorization data.

10. 7
12. (original) The cryptographic key split combiner of claim ~~9~~, wherein said token split generator includes means for generating a random sequence based on the label data.

B1 11. 7
13. (original) The cryptographic key split combiner of claim ~~9~~, wherein said token split generator includes means for generating a pseudorandom sequence based on the label data.

12. 7
14. (original) The cryptographic key split combiner of claim ~~9~~, wherein said token split generator includes means for generating a key split based on the label data and on organization data.

13. 7
15. (original) The cryptographic key split combiner of claim ~~9~~, wherein said token split generator includes means for generating a key split based on the label data and on static data.

14. 13
16. (original) The cryptographic key split combiner of claim ~~15~~, further including means for updating the static data.

B

15. 14
~~17~~. (original) The cryptographic key split combiner of claim ~~16~~, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

16, 1
~~18~~. (previously presented) The cryptographic key split combiner of claim ~~3~~, wherein said plurality of key split generators includes a console split generator for generating a console key split based on maintenance data.

B1

17, 16
~~19~~. (original) The cryptographic key split combiner of claim ~~18~~, wherein said console split generator includes means for generating a random sequence based on the maintenance data.

18. 16
~~20~~. (original) The cryptographic key split combiner of claim ~~18~~, wherein said console split generator includes means for generating a pseudorandom sequence based on the maintenance data.

19, 16
~~21~~. (original) The cryptographic key split combiner of claim ~~18~~, wherein said console split generator includes means for generating a key split based on previous maintenance data and on current maintenance data.

20. 16
~~22~~. (original) The cryptographic key split combiner of claim ~~18~~, wherein said console split generator includes means for generating a key split based on the maintenance data and on static data.

21. 20
~~23~~. (original) The cryptographic key split combiner of claim ~~22~~, further including means for updating the static data.

22, 21
~~24~~. (currently amended) The cryptographic key split combiner of claim ~~22~~ ~~23~~, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

B1
23.
~~25~~. (previously presented) The cryptographic key split combiner of claim ~~3~~, 1 wherein said plurality of key split generators includes a biometric split generator for generating a biometric key split based on biometric data.

24, 23
~~26~~. (original) The cryptographic key split combiner of claim ~~25~~, wherein said biometric split generator includes means for generating a random sequence based on the biometric data.

25. 23
~~27~~. (original) The cryptographic key split combiner of claim ~~25~~, wherein said biometric split generator includes means for generating a pseudorandom sequence based on the biometric data.

26. 23
~~28~~. (original) The cryptographic key split combiner of claim ~~25~~, wherein said biometric split generator includes means for generating a key split based on biometric data vectors and on biometric combiner data.

B

27. 23
~~29~~. (original) The cryptographic key split combiner of claim ~~25~~, wherein said biometric split generator includes means for generating a key split based on the biometric data and on static data.

28. 27
~~30~~. (original) The cryptographic key split combiner of claim ~~29~~, further including means for updating the static data.

B1

29. 28
~~31~~. (original) The cryptographic key split combiner of claim ~~30~~, wherein the means for updating the static data includes means for modifying a prime number divisor of the static data.

30. 1
~~32~~. (previously presented) The cryptographic key split combiner of claim ~~3~~, wherein the cryptographic key is a stream of symbols.

31. 1
~~33~~. (previously presented) The cryptographic key split combiner of claim ~~3~~, wherein the cryptographic key is at least one symbol block.

32. 1
~~34~~. (previously presented) The cryptographic key split combiner of claim ~~3~~, wherein the cryptographic key is a key matrix.

35. (canceled)

36. (canceled)

37. (previously presented) A process for forming cryptographic keys, comprising:

generating a plurality of cryptographic key splits from seed data; and

randomizing the cryptographic key splits to produce a cryptographic key;

wherein generating a plurality of cryptographic key splits includes generating a random key split based on reference data; and

wherein generating a random key split includes generating a random sequence based on the reference data.

38. (previously presented) The process of claim 37, wherein generating a random key split includes generating a pseudorandom sequence based on the reference data.

39. (previously presented) The process of claim 37, wherein generating a random key split includes generating a key split based on the reference data and on chronological data.

40. (previously presented) The process of claim 37, wherein generating a random key split includes generating a key split based on the reference data and on static data.

41. (original) The process of claim 40, further including updating the static data.

38. 37
~~42~~. (original) The process of claim ~~41~~, wherein updating the static data includes modifying a prime number divisor of the static data.

~~39~~. 33
~~43~~. (previously presented) The process of claim ~~37~~, wherein generating a plurality of cryptographic key splits includes generating a token key split based on label data.

B1

40. 39
~~44~~. (original) The process of claim ~~43~~, further comprising reading the label data from a storage medium.

41. 39
~~45~~. (original) The process of claim ~~43~~, wherein the label data includes user authorization data.

42. 39
~~46~~. (original) The process of claim ~~43~~, wherein generating a token key split includes generating a random sequence based on the label data.

43. 39
~~47~~. (original) The process of claim ~~43~~, wherein generating a token key split includes generating a pseudorandom sequence based on the label data.

44. ~~39~~ 39
~~48~~. (original) The process of claim ~~43~~, wherein generating a token key split includes generating a key split based on the label data and on organization data.

45.
~~49~~. (original) The process of claim ~~43~~ 39, wherein generating a token key split includes generating a key split based on the label data and on static data.

46.
~~50~~. (original) The process of claim ~~49~~ 45, further including updating the static data.

47.
~~51~~. (original) The process of claim ~~50~~ 46, wherein updating the static data includes modifying a prime number divisor of the static data.

48.
~~52~~. (previously presented) The process of claim ~~37~~ 33, wherein generating a plurality of cryptographic key splits includes generating a console key split based on maintenance data.

49 ~~50~~.
~~53~~. (original) The process of claim ~~52~~ 48, wherein generating a console key split includes generating a random sequence based on the maintenance data.

50.
~~54~~. (original) The process of claim ~~52~~ 48, wherein generating a console key split includes generating a pseudorandom sequence based on the maintenance data.

51.
~~55~~. (original) The process of claim ~~52~~ 48, wherein generating a console key split includes generating a key split based on previous maintenance data and on current maintenance data.

52. 48
~~56~~. (original) The process of claim ~~52~~, wherein generating a console key split includes generating a key split based on the maintenance data and on static data.

53. 52
~~57~~. (original) The process of claim ~~56~~, further including updating the static data.

54. 53
~~58~~. (currently amended) The process of claim ~~56~~ ~~57~~, wherein the updating the static data includes modifying a prime number divisor of the static data.

55. 33
~~59~~. (previously presented) The process of claim ~~37~~, wherein generating a plurality of cryptographic key splits includes generating a biometric key split based on biometric data.

56. 55
~~60~~. (original) The process of claim ~~59~~, wherein generating a biometric key split includes generating a random sequence based on the biometric data.

57. 55
~~61~~. (original) The process of claim ~~59~~, wherein generating a biometric key split includes generating a pseudorandom sequence based on the biometric data.

58. 55
~~62~~. (original) The process of claim ~~59~~, wherein generating a biometric key split includes generating a key split based on biometric data vectors and on biometric combiner data.

59. 55
63. (original) The process of claim 59, wherein generating a biometric key split includes generating a key split based on the biometric data and on static data.

60. 59
64. (original) The process of claim 63, further including updating the static data.

61. 60
65. (previously presented) The process of claim 64, wherein updating the static data includes modifying a prime number divisor of the static data.

B1

66. (canceled)

63. 62
67. (previously presented) The cryptographic key of claim 70, including a stream of symbols.

64. 62
68. (previously presented) The cryptographic key of claim 70, including at least one symbol block.

65. 62
69. (previously presented) The cryptographic key of claim 70, including a key matrix.

62.
70. (previously presented) A cryptographic key, formed by the process of claim

33
37.